Mobile Banking App is HERE!

Union Bank

March 2022

8 Tips for Safe Online Shopping

Online shopping can be convenient, cost-effective and safe—provided you take certain precautions before making your purchase. Best practices include:\

Only trust encrypted websites
Not all e-commerce sites provide the ideal conditions for safe online shopping. It's important to limit your shopping to encrypted websites, and only conduct transactions when you're on a trusted WiFi network. "Look for a padlock symbol on the URL bar, as well as next to your WiFi network's name," advises Satish Kanwar, product director at Shopify.ca. "Following these steps is the best way to ensure that your personal information is being transferred in the safest way possible."

Protect your personal information
It's normal for online retailers to request additional details and preferences to make your online shopping experience more personalized. However, if they ask for too much information—like your social security number, for instance—that's a definite red flag.

Create unique passwords for each website
Avoid using the same password for every online shopping site you frequent. "That way, if your login information gets stolen on one website, your other accounts likely won't get compromised," says Kanwar.

Look for the 'S'
Any time you input personal or credit card information into a website, ensure the page is secured. Kanwar says that the quickest way to check for this is in the URL. "The website URL should start with https:// (rather than http://) and should have a padlock symbol to indicate that the page is secure."

Be wary of dream deals
Kanwar warns consumers to regard sale-of-the-century price tags with a healthy dose of skepticism. "When items are priced significantly lower than they should be, that should raise a flag about the legitimacy and authenticity of the website," he says. "Low prices are enticing, but if it's too good to be true, it usually is."

Look for customer service information
Safe online shopping sites have their toll-free customer service line or email address readily available. Kanwar also recommends reading over the website's refunds and exchanges policies: openness about

Continued on Page 2

Member FDIC

EQUAL HOUSING LENDER

Middlebourne Office
103 Dodd Street Middlebourne, WV 26149
304-758-2191

Sistersville Office
700 Wells Street Sistersville, WV 26175
304-652-3511

St. Marys Office
401 Second Street St. Mary's, WV 26170
304-684-2427

Hundred Office
3924 Hornet Hwy, Hundred WV 26575
304-775-2265

Ellenboro Office
90 Main Street Ellenboro, WV 26346
304-869-3232

Harrisville Office
1500 E. Main Street Harrisville, WV 26362
304-643-2974

Pennsboro Office
214 Masonic Ave. Pennsboro, WV 26415
304-659-2964

Marietta-Loan Production
Kroger Plaza 19 Acme Street Marietta, OH 45750
740-374-0010

This is not a full service location. Deposits/withdrawals cannot be processed at this location.

New Martinsville Office
638 N SR 2 New Martinsville, WV 26155
304-455-2967

these conditions is often a good indicator of credibility.

Don't click on untrusted pop-up ads
While it's common practice for retailers to use pop-up ads for e-newsletters, promotions and flyers, Kanwar warns consumers to keep an eye out for phishing scams. "Pesky pop-ups are a way for scammers to lure or confuse online shoppers," he says. "Make sure to have an ad-blocker installed when shopping on unfamiliar websites to avoid getting phished."

Check your credit card statement
Keep a close tab on your credit card statements, even after you've received your purchased item. "It's always smart to ensure that there were no hidden charges tacked on, or unfamiliar names deducting from your account," Kanwar suggests.

Source: ***Simone Castello, readersdigest.ca, Updated: Oct. 26, 2021***

3 Times You Should Never "Accept Cookies" on a Site

Cookies are everywhere online, but should you allow them into your browsing life?
Cookie-consent pop-ups are one of the biggest annoyances on the Internet. Almost every site you visit has a notice saying, "This website uses cookies to improve your experience. Do you agree?" or something similar. Typically, we click "yes" or "agree" without even thinking about it because we're eager to get to the content. But should we? Not necessarily.

What are cookies, exactly?
Before we delve into the dos and don'ts of cookie consent, here's a little refresher on this Web tool: Cookies are essentially information collectors and trackers in the form of small text files stored on your browser by the sites you visit. Some are useful. For example, a cookie saved on your browser makes it so you don't have to re-enter your log-in information every time you visit one of your favorite websites. Cookies can also remember your shopping preferences so that you get a personalized experience when you visit the website. Others, however, track how you use a website, how often you go there, your IP address, your phone number, what types of things you look at and buy, and other information you may not want to share.

Do you have to accept cookies?
Many companies have you click "yes" so that they're compliant with current privacy laws. This means that once you click, you've given the company permission to use your information as they see fit without the worry of legal backlash. Most of the time, cookies are no big deal. There are a few occasions, though, where you should decline cookies. Don't worry—if you find yourself in a situation where you need to decline or simply want to decline for whatever reason, most websites will work just fine without collecting your information. With that said, here's when saying no to the cookies is a good idea.

Sketchy sites
Beware when you're on an unencrypted website (these websites will have an unlocked lock icon by the web address) while using a public Wi-Fi network. The information collected by cookies can be intercepted by hackers because there isn't any security to stop them. Your best bet when borrowing Wi-Fi from your local coffee shop or fast-food joint is to use your browser's private or incognito mode. While in this mode, cookies aren't collected by default (though you can manually turn off cookie blocking on some browsers), no matter where your Internet journeys take you.

Third-party cookies
If the cookie-consent pop-up mentions third-party cookies, click "decline." Accepting gives the website the right to sell your browsing behavior to a data broker. The broker then combines your behavior on one website with information from other websites and builds an extremely detailed profile of you as a consumer. "The broker then sells that profile to other third parties who want to market to people like you," says Harry Maugans, CEO of Privacy Bee, a proactive privacy management tool for consumers. "As you can imagine, this chain extends infinitely. Once you lose control of your personal data, it gets packaged and repackaged in all kinds of ways. It's scary but true."

According to Maugans, some third-party cookies are even nefarious. You could become a victim of "cookie stealing" or "session hijacking." This is when a hacker gains access to a browser and mimics users to be able to steal cookies from that browser. This can put you at risk of identity theft if hackers manage to steal cookies that store your personal information or credit card information.

If you're worried that you might accidentally accept third-party cookies, there's an easy way to make things fool-proof. Go into your browser and choose to allow only required cookies or "first party" cookies. These cookies are the helpful ones mentioned earlier and are usually only used by the website you're visiting.

When you're using private information
If you don't feel comfortable sharing the information you're using or accessing on a website with a stranger, don't use cookies on that site. According to Jeremy Tillman, president of the privacy company Ghostery, you should avoid cookies on sites where you do your banking, access your medical information, or use other private information.

If you're afraid that you've already accepted cookies on websites where you wouldn't want your information gathered, go into your browser and use the "clear cookies" option. This will prevent sites from collecting your information in the future, as long as you decline the next time a site asks you to accept its cookies.

Source: ***Alina Bradford, RD.com, Updated: Sep. 23, 2021***

What is a Botnet?

A botnet is a network of computers infected with malware that are controlled by a bot herder. The bot herder is the person who operates the botnet infrastructure and uses the compromised computers to launch attacks designed to crash a target's network, inject malware, harvest credentials or execute CPU-intensive tasks. Each individual device within the botnet network is called a bot.

How are Botnets Controlled?

Bot herders control their botnets through one of two structures: a centralized model with direct communication between the bot herder and each computer, and a decentralized system with multiple links between all the infected botnet devices.

How Does a Botnet Work?

The stages of creating a botnet can be simplified into these steps:

1. *Expose*
2. *Infect and Grow*
3. *Activate*

In stage 1, the hacker will find a vulnerability in either a website, application, or user behavior in order to expose users to malware.

In stage 2, victims' devices are infected with malware that can take control of their devices. The initial malware infection allows hackers to create zombie devices using techniques like web downloads, exploit kits, popup ads, and email attachments.

In stage 3, when the bot herder has infected a sufficient amount of bots, they can then mobilize their attacks. The zombie devices will then download the latest update to receive its order. The bot then proceeds with its orders and engages in malicious activities. The bot herder can continue to remotely manage and grow their botnet to carry out various malicious activities.

Types of Botnet Attacks

Once an adversary is in control of a botnet, the malicious possibilities are extensive. A botnet can be used to conduct many types of attacks, including:

1. Phishing

Botnets can be used to distribute malware via phishing emails.

2. Distributed Denial-of-Service (DDoS) attack

During a DDoS attack, the botnet sends an overwhelming number of requests to a targeted server or application, causing it to crash.

3. Spambots

Spambots harvest emails from websites, forums, guestbooks, chat rooms and anyplace else users enter their email addresses. Once acquired, the emails are used to create accounts and send spam messages. Over 80 percent of spam is thought to come from botnets.

How to Protect Against Botnets

To prevent your devices from becoming part of a botnet, it is recommended that your organization consider the following recommendations:

- Regular security awareness training programs that teach users/employees to identify malicious links.
- Always keep your software updated to decrease the chances of a botnet attack exploiting weaknesses in the system.
- Use two-factor authentication to prevent botnet malware from breaking into devices and accounts if a password has been compromised.
- Update passwords across all devices, especially the privacy and security options on those that connect device-to-device or to the internet.
- A quality antivirus solution that is kept up to date and scans the network regularly.
- Deploy an intrusion detection system (IDS) across your network.
- An endpoint protection solution that includes rootkit detection capability and that can detect and block malicious network traffic.

Source: Crowdstrike, January 12, 2022